UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF TEXAS

ERIC L. ELLIS, Plaintiff, vs. CARGILL MEAT SOLUTIONS, AND ULTIMATE KRONOS GROUP (UKG) Defendant	Case No.: 4:22-CV- 00864

PLAINTIFF'S AMENDED COMPLAINT WITH JURY DEMAND

INTRODUCTION

NOW COMES Eric L. Ellis, Plaintiff, complaining of Defendants, CARGILL MEAT SOLUTIONS and ULTIMATE KRONOS GROUP (UKG) for cause would show this Honorable Court as follows:

This case arises out of Cargill's discriminatory treatment of the Plaintiff in violation of federal and applicable state civil rights laws. Cargill has not served Plaintiff with a responsive pleading. Having satisfied all administrative prerequisites and prior to being served with a responsive pleading, Plaintiff now files this Amended Complaint.

This case also arises out of the Defendants' failure to safeguard the personal identifying information of the Plaintiff Eric Ellis.

Plaintiff Eric Ellis brings this action against UKG for its failure to implement and maintain reasonable security procedures and practices with respect to the sensitive and confidential personal information UKG obtains

from its customers' employees. Plaintiff Eric Ellis's employer Cargill Meat Solution whom at all times relevant to this action was an active customer of Defendant UKG.

UKG is one of the world's largest workforce management software companies. The company collects, stores, and processes data for thousands of companies and millions of workers. UKG's clients broadly range between corporate and public organizations.

As a result of its lack of adequate security measures, UKG was attacked by hackers who launched a ransomware attack on UKG's timekeeping system, Kronos Private Cloud, on or around December 11, 2021.

The data breach exposed millions of workers' sensitive and confidential personal identifying information ("PII") to cybercriminals.

To make matters worse, the attack also crippled timekeeping and payroll systems, resulting in workers not being paid, being paid late, or being paid incorrectly.

The timing of the data breach could not have come at a worse time, leaving many employees to worry over their privacy and paychecks during the peak of the holiday season as well as the latest surge of the COVID-19 pandemic.

As a result of UKG's payroll services going offline, all Cargill Meat Solutions employees were delayed payment of their paychecks.

All Cargill's employees were forced to find alternative sources of income to pay their bills, mortgages, and necessities, again during the midst of the holiday season.

Even after Cargill got around to distributing paychecks to its employees, many Cargill's employees were either paid inaccurately and/or not at all.

In the months following the data breach, all Cargill employees have had to invest significant time and expense into determining the amount of any unpaid wages, bonuses, and/or paid time off.

In addition to their paychecks being affected, Plaintiff's and all Cargill employees' sensitive and confidential PII was obtained by unauthorized hackers and sold on the dark web. As a result, Cargill employees not only have to deal with the loss of wages and the resulting consequences, but also have had to invest time and money into securing their personal and financial information.

Plaintiff brings this action to redress these injuries, on his own behalf.

A. NATURE OF ACTION

This is an action under Title VII of the Civil Rights Act of 1964, and Title I of the Civil Rights Act of 1991, to correct unlawful employment practices on the basis of sexual orientation and to provide appropriate relief to Eric Ellis whom was subjected to a sexually hostile work environment, sex-based discrimination and constructive discharge. Plaintiff, Eric Ellis also alleges that he was subjected to disparate treatment falsely accusing Eric Ellis of wrongdoing, issuing conflicting work orders in repeated attempts to anger and encourage insubordination, closely and unnecessarily scrutinizing work, and issuing groundless reprimands. This complaint further alleges that the harassment was carried out with the intent of segregating Homosexual and

Heterosexual employees, employees who made complaints of discrimination, opposed discriminatory treatment of co-workers, and/or participated in reporting or serving as witnesses to grievances of discrimination. Eric Ellis was compelled to resign because of the intolerable work environment created by Cargill Meat Solutions.

Eric Ellis also brings this action against Cargill for FLSA violations, and other claims stemming from a data breach caused by one of its service providers Ultimate Kronos Group (UKG).

COVERAGE UNDER THE FLSA

At all relevant times, Cargill Meat Solutions was an employer of Eric Ellis within the meaning of Section 3(d) of the FLSA, 29 U.S.C. § 203(d).

At all relevant times, Cargill Meat Solutions was and is an employer of Eric Ellis within the meaning of Section 3(d) of the FLSA, 29 U.S.C. § 203(d).

Cargill Meat Solutions was and is part of an enterprise within the meaning of Section 3(r) of the FLSA, 29 U.S.C. § 203(r).

During at least the last three years, Cargill Meat Solutions has had gross annual sales in excess of $500,000.

Cargill Meat Solutions was and is part of an enterprise engaged in commerce or in the production of goods for commerce within the meaning of the FLSA, 29 U.S.C. § 203(s)(1).

Cargill Meat Solutions employs many workers, including Eric Ellis, who are engaged in commerce or in the production of goods for commerce and/or who handle, sell, or otherwise work on goods or materials that have been moved in or produced for commerce by any person.

The goods and materials handled, sold, or otherwise worked on by Ellis, and other Cargill Meat Solutions' employees and that have been moved in interstate commerce include, but are not limited to, ready to eat foods and their component parts.

B. PARTIES

At all relevant times Plaintiff Eric L. Ellis was a male adult of sound mind and a resident of 637 Yarborough St Bossier City, La 71111.

Defendant Cargill Meat Solutions at all relevant times, has continuously

been and is now doing business in the State of Texas and has continuously had at least 200 employees.

At all relevant times, Defendant, Cargill Meat Solutions, has continuously been an employer engaged in an industry affecting commerce under Section 701(b), (g) and (h) of Title VII, 42 U.S.C. §2000e-(b), (g) and (h).

Defendant Ultimate Kronos Group is a company is an American multinational technology company. It provides workforce management and human resource management services to Cargill Meat Solutions. At all relevant times in this lawsuit, Ultimate Kronos Group was acting as a service provider for Cargill Meat Solutions.

Defendant UKG, Inc. is a corporation formed under the laws of the State of Delaware, with dual corporate headquarters in Weston, Florida and Lowell, Massachusetts.

C. JURISDICTION AND VENUE

This Court has original jurisdiction over the subject matter of this suit pursuant to 18 U.S.c. § 1964(c), 28 U.S.c. § 1331, §1332, §1343 and 42 U.S.C. § 2000e-5f(1).

This Court has supplemental jurisdiction over the subject matter pursuant to 28 U.S.C. § 1367(a).

Venue is proper because a substantial part of the events giving rise to the claims occurred in this judicial district. See 28 U.S.C. § 1391(b)(2).

This Court is empowered to issue a declaratory judgment and further relief pursuant to 28 U.S.C. § 2202.

The Court has general personal jurisdiction over UKG because, at all relevant times, UKG has had systematic and continuous contacts with the

State of Texas. UKG is registered to do business in Texas with the Texas Secretary of State. UKG regularly contracts with a multitude of businesses and organizations in Texas to provide continuous and ongoing human resource services, including timekeeping and payroll services.

This Court has specific personal jurisdiction over UKG because Plaintiff's claims arise from UKG's specific contacts with the State of Texas– namely, UKG's provision of payroll and other human resource services to a multitude of companies in Texas, UKG's failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent connection with such services.

STATEMENT OF FACTS FOR WORK PLACE DISCRIMINATION

More than thirty days prior to the institution of this lawsuit, Eric Ellis filed charges with the Equal Employment Opportunity Commission alleging violations of Title VII of the Civil Rights Act of 1964, by the Defendant, Cargill Meat Solutions. All conditions precedent to the institution of this lawsuit have been fulfilled.

During the employment of Eric Ellis, the Defendant has engaged in unlawful employment practices in violation of Section 703(a)(1) of Title VII, 42 U.S.C. § 2000e2(a)(1) by subjecting Eric Ellis to a sexually hostile work environment, discriminating against him on account of his sexual orientation, retaliating against him for complaining of the working conditions and constructively discharging him. Specifically, Cargill Meat Solutions subjected Ellis to a sexually hostile work atmosphere in that he was constantly and repeatedly subjected to sexually explicit remarks, demeaning hateful homosexual remarks, frequent heterosexual sex scenes (from movies and tv shows) that appeared in multiple breakrooms at

Cargill and violent vandalism, resulting in his constructive discharge from the position.

The result of the foregoing practices has been to deprive Eric Ellis of equal employment opportunities because of his sexual orientation. Defendant Cargill Meat Solutions maintained a hostile work environment in its Fort Worth, Texas facility wherein homosexual employees were falsely accused of wrongdoing, issued conflicting work orders in repeated attempts to anger and encourage insubordination, subjected to unnecessary scrutiny of his work, and made the target of groundless reprimands with the intent of humiliating the homosexual employee because of his sexual orientation. Defendant Cargill Meat Solutions subjected homosexual employees to disparate treatment at its Fort Worth, Texas facility by intentionally targeting the homosexual employees for reprimands, extra job duties and false accusations of wrongdoing. Other similarly situated Heterosexual employees, who were actually guilty of misconduct or infractions, were not disciplined, much less targeted for termination, disciplinary actions, or discharged, due to their poor work quality. The disparate treatment in the terms and conditions of their employment forced Eric Ellis to resign;

Defendant Cargill Meat Solutions retaliated against Eric Ellis, whom brought allegations of discrimination, opposed discriminatory treatment of coworkers, and/or participated in reporting or serving as witnesses to grievances of discrimination by subjecting him to reprimands, extra job duties, increased scrutiny, false accusations of wrongdoing and denial of due process. Defendant Cargill Meat Solutions also breached its de facto obligation of good faith and fair dealing in managing its own employees and following its own policies. Defendant Cargill Meat Solutions has without reasonable and proper cause conducted itself in a way that destroyed the

relationship of trust and confidence.

Members of Defendant Cargill Meat Solutions's management, at its Fort Worth, Texas facility, allowed the discrimination complained of in all paragraphs of this complaint to go unaddressed despite repeated complaints by Eric Ellis.

Due to the harassment, Eric Ellis was forced to resign. Defendant Cargill Meat Solutions subjected Homosexual employees to disparate treatment at its Fort Worth, Texas facility by intentionally targeting the Homosexual employees for reprimands, extra job duties and false accusations of wrongdoing. Other similarly situated Heterosexual employees, who were actually guilty of misconduct or infractions, were not disciplined, much less targeted for termination, or discharged, due to their poor work quality. The disparate treatment in the terms and conditions of their employment forced several Homosexual employees to resign;

The unlawful employment practices complained of in all paragraphs of this complaint above were intentional.

The unlawful employment practices complained of in all paragraphs of this complaint above were done with malice or with reckless indifference to the federally protected rights of Eric Ellis.

CONDITIONS PRECEDENT

All conditions precedent to jurisdiction have occurred or been complied with: a charge of discrimination was filed with the Equal Employment Opportunity Commission within three hundred days of the acts complained of herein and Plaintiff's Complaint is filed within ninety days of Plaintiff's receipt of the Equal Employment Opportunity Commission's issuance of a right to sue letter.

FACTUAL ALLEGATIONS AGAINST UKG

Plaintiff has worked as a Food Safety Quality Representative for Cargill Meat Solutions.

Cargill uses Kronos Privates Cloud to process payroll. On December 12, 2021, Cargill notified its employees that as a result of a malware attack on UKG's system, Cargill's payroll software was offline. As a direct and foreseeable result of UKG's negligent failure to implement and maintain reasonable data security procedures and practices and the resultant breach of its systems, Cargill's timekeeping and payroll systems became crippled and remained completely offline for weeks following the data breach. Cargill lacked an adequate contingency plan to accurately pay workers and was forced to switch to manually inputting payroll.

On December 13, 2021, Cargill notified its employees that employees would need to maintain and submit "manual timesheets" for time worked following the data breach. Cargill further instructed it employees that for payroll accumulated before December 10, 2021, Cargill would need to utilize employees' employment status to process payroll. Cargill instructed employees who had concerns with this method of calculating payroll to contact Cargill.

Plaintiff was delayed payment of his paycheck following the data breach. Following the data breach, Plaintiff's payroll was scheduled to be processed by December 17, 2021. The resultant shutdown of UKG's payroll services caused each Cargill employee, including Plaintiff, to not receive his paycheck until after Christmas. Plaintiff had to endure weeks without payment while working during the Omicron surge in the midst of the holiday season.

Plaintiff has lost time and expenses from having to mitigate the consequences of the delay in payment of his paychecks.

Plaintiff also had his PII, including but not limited to his name, company name, address, email address, time and attendance and schedule information, and Social Security Number, exposed as a result of UKG's negligent failure to safekeep his information.

As a direct and foreseeable result of UKG's negligent failure to implement and maintain reasonable data security procedures and practices and the resultant breach of its systems, Plaintiff also suffered harm in that his sensitive PII has been exposed to cybercriminals and they now have an increased risk and fear of identity theft and fraud.

Since the data breach, Plaintiff has received on average, per day 5-6 spam calls to his cell phone and countless spam e-mails. Further, shortly after the data breach, Plaintiff received a notification from his credit card company that his Social Security number had been discovered on the dark web. Upon information and belief, Plaintiff's Social Security number, cell phone number and e-mail address were exfiltrated by the hackers who obtained unauthorized access to Plaintiff's' PII.

Social Security numbers are among the most sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your

number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

Accordingly, Plaintiff Eric Ellis has suffered harm in the form of increased fear and risk of identity theft and fraud resulting from the data breach.

UKG Inc. (an acronym for Ultimate Kronos Group) is a workforce management software company that provides human resource services, including timekeeping and payroll services, to companies across the globe. Among the many products and services that it offers, UKG provides software known as the "Kronos Private Cloud" and "UKG Workforce Central," which are timekeeping and payroll services.

UKG was formed as a result of a $22 billion merger in 2020 between Ultimate Software and Kronos. The company has 13,000 employees across the globe, and amidst a global pandemic, was able to generate over $3 billion in revenue in its first year of business. It is one of the largest cloud computing companies in the world and a leading global provider of workforce management services.

UKG provides its timekeeping and payroll services to a multitude of companies and organizations, including Cargill Meat Solutions.

In connection with those services, UKG collects, stores, and processes sensitive personal data for thousands of companies and millions of workers. Prior to the data breach, UKG had enacted a privacy notice in which it states UKG collects PII of individuals from a variety of sources, including directly from its customers and their employees. The privacy notice contains a section entitled "Customers' Information [and the Information of Their Employees and Job Applicants]", which states that UKG collects data including, but not limited to "name, company name, address, email address, time and attendance and schedule information, and Social Security Numbers."

UKG Job Applicants and Employees

How Do We Use Your Personal Information?

We use PI of our job applicants and employees for legitimate human resource business purposes, such as:

- Payroll administration;
- Filling open employment positions;
- Maintaining accurate benefits records;
- Complying with governmental reporting requirements;
- Performance management;
- Provision of company network access;
- Authentication of individuals; and
- Security, health and safety management.

Customers' Information (and the Information of Their Employees)

How Do We Use Your Personal Information?

We use your PI to provide you with services, which UKG is contractually obliged to provide to you, to improve these services or communicate with you about our products or services. For employees of customers who use UKG terminals with a biometric or finger scanning device for employee timekeeping, please see the Biometric Data Privacy section of this Notice.

UKG also collects banking information in connection with its provision of direct deposit payroll processes as well as employee identification numbers. For example, under "Use of Personal Information", under the subsection titled "Customers' Information (and the Information of Their Employees)," UKG's privacy notice states UKG uses the PII of its customers' employees to provide its customers with services.

UKG's services, among other things, allows its customers to ensure accurate, on-time pay and to quickly generate payroll documents, such as paychecks and direct-deposit files.

On December 13, 2021, UKG posted an announcement regarding the data breach on its website. The announcement confirmed that that a ransomware attack was made on UKG's Kronos Private Cloud. The Kronos Private Cloud includes Defendant's UKG Workforce Central, UKG TeleStaff, Healthcare Extensions, and Banking Scheduling Solutions. Defendant confirmed that as a result of the attack, Kronos Private Cloud solutions was offline.

UKG advised its customers "that it may take up to several weeks to restore system availability," and that as such, the company "strongly recommends that [customers] evaluate and implement alternative business continuity protocols related to the affected UKG solutions."

On December 17, 2021, Defendant then posted on its website "New Questions & Answers for Impacted and Non-Impacted Customers" that, among other things, stated the following question and answer:

Precisely what information was accessed or exposed? Our investigation is ongoing and we are working diligently to determine if customer data has been compromised.

On December 28, 2021, UKG finally acknowledged the potential exposure of sensitive employee PII as follows:

On January 22, 2022, UKG posted an update to its website stating that "[b]etween January 4 and January 22, all affected customers in the Kronos Private Cloud were restored with safe and secure access to their core time, scheduling, and HR/payroll capabilities. We are now focused on

the restoration of supplemental features and non-production environments and are extraordinarily grateful for the patience and partnership our customers have shown.

To date, UKG has not confirmed what information was stolen.

Upon information and belief, the hackers responsible for the data breach stole the PII of all employees of UKG's customers.

The FBI created a technical guidance document for Chief Information Officers and Chief Information Security Officers that complies already existing federal government and private industry best practices and mitigation strategies to prevent and respond to ransomware attacks. The document is titled How to Protect Your Networks from Ransomware and states that on average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. Yet, there are very effective prevention and response actions that can significantly mitigate the risks.

Preventative measure include:

• Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

• Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

• Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

• Configure firewalls to block access to known malicious IP addresses.

• Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system. • Set anti-virus and anti-malware programs to conduct regular scans automatically. • Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

• Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

• Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

• Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

• Consider disabling Remote Desktop protocol (RDP) if it is not being used. • Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

• Execute operating system environments or specific programs in a virtualized environment.

• Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

(https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view)

UKG could have prevented the data breach by properly utilizing best practices as advised by the federal government.

UKG's failure to safeguard the PII of employees of Defendant's customers is exacerbated by the repeated warnings and alerts from public and private institutions, including the federal government, directed to protecting and securing sensitive data. Experts studying cyber security routinely identify companies such as UKG that collect, process, and store massive amounts of data on cloud-based systems as being particularly vulnerable to cyberattacks because of the value of the PII that they collect and maintain. Accordingly, UKG knew or should have known that it was a prime target for hackers.

According to the 2021 Thales Global Cloud Security Study, more than 40% of organizations experienced a cloud-based data breach in the previous 12 months. Yet, despite these incidents, the study found that nearly 83% of cloud-based businesses still fail to encrypt half of the sensitive data they store in the cloud.

Upon information and belief, Kronos did not encrypt Plaintiff's PII involved in the data breach.

Defendant's knowledge that it was a target of hackers is further underscored by the massive number of ransomware attacks on payroll companies such as UKG.

Defendant's knowledge that it was a target of hackers is further underscored by the massive number of ransomware attacks on payroll companies such as UKG.

In March of 2021, PrismHR, a Massachusetts-based payroll company that services over 80,000 organizations, suffered a massive outage after suffering a cyberattack on its payroll cloud-based system.

In January of 2021, 6,000 employees' PII was stolen during a ransomware attack on Arup's, a UK-based third-party payroll provider.

In May of 2020, Interserver, a payroll vendor for Britain's Ministry of Defense, was hacked. The hackers obtained the sensitive information of up to 100,000 past and current employees.

In February of 2020, the Phoenix Pay System fell prey to a data breach exposing the PII of more than 69,000 Canadian federal employees.

Despite knowing the prevalence of data breaches, UKG failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. UKG has the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized breaches. UKG failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures to ensure vulnerabilities were avoided or remedied and that Plaintiff's data was protected.

Plaintiff's personal information was exposed as a result of the Kronos Data Breach.

Plaintiff's paychecks were paid late, inaccurately, and/or not at all as a result of the Kronos Data Breach.

Defendants failed to reasonably protect Plaintiff's PII from unauthorized third-party hackers.

CLAIMS FOR RELIEF AGAINST CARGILL MEAT SOLUTIONS

COUNT I

RESPONDEAT SUPERIOR

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

Whenever in this complaint it is alleged that the Defendant did any act or thing, it is meant that the Defendant's officers, agents, servants, employees, or representatives did such act and/or that at that time such act was done, it was done with the full authorization or ratification of the Defendant or was done in the normal and routine course and scope of employment of Defendant, officers, agents, servants, employees, or representatives.

COUNT II

RACE AND SEX DISCRIMINATION

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

Defendant, Cargill Meat Solutions, intentionally engaged in unlawful employment practices involving Plaintiff because of his race and sexual orientation.

Defendant, Cargill Meat Solutions, intentionally discriminated against Plaintiff in connection with the compensation, terms, conditions and

privileges of employment or limited, segregated or classified Plaintiff in a manner that would deprive or tend to deprive him of any employment opportunity or adversely affect his status because of Plaintiff's race and sex in violation of 42 U.S.C. Section 2000e (2)(a).

Defendant, Cargill Meat Solutions, intentionally classified Plaintiff in a manner that deprived him of an equal employment opportunity that was provided to other non-black employees similarly situated in violation of 42 U.S.C. Section 2000e (2)(a).

Defendant, Cargill Meat Solutions, also violated Plaintiffs rights under 42 U.S.C. Section 1981.

COUNT III

HOSTILE WORK ENVIRONMENT

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

Defendant violated Title VII of the Civil Rights Act of 1964 by creating a hostile work environment by repetitive use of racial slurs and also by retaliating against him because of his race and sexual orientation.

COUNT IV

INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS BY CARGILL MEAT SOLUTIONS

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

Defendant Cargill Meat Solutions intentionally or recklessly harassed the plaintiff in the form of racial slurs. Defendant's conduct was extreme and outrageous and proximately caused Plaintiff severe emotional distress. Plaintiff suffered damages for which Plaintiff herein sues.

STATEMENT OF FACTS FOR FLSA VIOLATIONS

Cargill Meat Solutions manufactures, processes and distributes cooked food products.

Many of Cargill Meat Solutions's employees are non-exempt hourly and salaried workers.

Since at least 2021, Cargill Meat Solutions has used timekeeping software and hardware operated and maintained by Kronos.

On or about December 11, 2021, Kronos was hacked with ransomware.

The Kronos hack interfered with the ability of its customers, including Cargill Meat Solutions, to use Kronos's software and hardware to track hours and pay employees.

Since the onset of the Kronos hack, Cargill Meat Solutions has not kept accurate track of the hours that Ellis have worked.

Instead, Cargill Meat Solutions has used various methods to estimate the number of hours Ellis work in each pay period.

For example, Cargill Meat Solutions issued paychecks based on scheduled hours or estimated hours, or simply duplicated paychecks from pay periods prior to the Kronos hack.

This means that employees who were non-exempt and worked overtime were in many cases paid less than the hours they worked in the workweek, including overtime hours.

Even if certain overtime hours were paid, the pay rate would be less than the full overtime premium. Many employees were not even paid their non-overtime wages for hours worked before 40 in a workweek.

Ellis is one of the employees affected by this decision by Cargill Meat Solutions and the resulting pay practice.

Instead of paying Ellis for the hours he actually worked (including overtime hours), Cargill Meat Solutions simply paid based on estimates of time or pay, or based upon arbitrary considerations other than Ellis's actual hours worked and regular pay rates.

In some instances, Ellis was paid portions of the overtime he worked, but the overtime rate he was paid was not at least 1.5 times his regular rate of pay, including required adjustments for shift differentials and non-discretionary bonuses.

In properly calculating and paying overtime to a non-exempt employee, the only metrics that are needed are: (1) the number of hours worked in a day or week, and (2) the employee's regular rate, taking into account shift differentials, non-discretionary bonuses, and other factors allowed under the law.

Cargill Meat Solutions knows it has to pay proper overtime premiums to nonexempt hourly and salaried employees.

Cargill Meat Solutions knows this because, prior to the Kronos hack, it routinely paid these workers for all overtime hours at the proper overtime rates.

Cargill Meat Solutions could have instituted any number of methods to accurately track and timely pay its employees for all hours worked.

Instead of accurately tracking hours and paying employees their overtime, Cargill Meat Solutions decided to arbitrarily pay these employees, without regard to the overtime hours they worked or the regular rates at which they were supposed to be paid.

Even if it did pay any overtime to affected employees, Cargill Meat Solutions did not take into account shift differentials and non-discretionary bonuses, such that the overtime premium Cargill Meat Solutions did pay, if any, was not the full overtime premium owed under the law based on the employees' regular rate.

It was feasible for Cargill Meat Solutions to have its employees and managers report accurate hours so they could be paid the full and correct amounts of money they were owed for the work they did for the company. But it chose not to do that.

In other words, Cargill Meat Solutions pushed the effects of the Kronos hack onto the backs of its most economically vulnerable workers, making sure that it kept the money it owed to those employees in its own pockets, rather than take steps to make sure its employees were paid on time and in full for the work they did.

Eric Ellis is just one of the many Cargill Meat Solutions employees who had to shoulder the burden of this decision by Cargill Meat Solutions.

Ellis was a non-exempt hourly employee of Cargill Meat Solutions.

Ellis regularly worked over 40 hours per week for Cargill Meat Solutions.

Ellis's normal, pre-Kronos hack hours are reflected in Cargill Meat Solutions records.

Since the Kronos hack, Cargill Meat Solutions has not paid Ellis for his actual hours worked each week.

Since the hack took place, Cargill Meat Solutions has not been accurately recording the hours worked by Ellis and its other workers.

Even when Cargill Meat Solutions has issued payment to Ellis for any overtime, the overtime is not calculated based on Ellis's regular rates, as required by federal law.

Cargill Meat Solutions was aware of the overtime requirements of the FLSA.

Cargill Meat Solutions nonetheless failed to pay the full overtime premium owed to certain non-exempt hourly and salaried employees, such as Ellis.

Cargill Meat Solutions's failure to pay overtime to these non-exempt workers was, and is, a willful violation of the FLSA.

The full overtime wages owed to Ellis became "unpaid" when the work for Cargill Meat Solutions was done—that is, on Ellis's regular paydays. E.g., Martin v. United States, 117 Fed. Cl. 611, 618 (2014); Biggs v. Wilson, 1 F.3d 1537, 1540 (9th Cir.1993); Cook v. United States, 855 F.2d 848, 851 (Fed. Cir. 1988); Olson v. Superior Pontiac–GMC, Inc., 765 F.2d 1570, 1579 (11th Cir.1985), modified, 776 F.2d 265 (11th Cir.1985); Atlantic Co. v. Broughton, 146 F.2d 480, 482 (5th Cir.1944); Birbalas v. Cuneo Printing Indus., 140 F.2d 826, 828 (7th Cir.1944).

At the time Cargill Meat Solutions failed to pay Ellis in full for his overtime hours by his regular paydays, Cargill Meat Solutions became liable for all prejudgment interest, liquidated damages, penalties, and any other damages owed under federal and Texas law.

In other words, there is no distinction between late payment and nonpayment of wages under federal law. Biggs v. Wilson, 1 F.3d 1537, 1540 (9th Cir.1993).

Even if Cargill Meat Solutions made any untimely payment of unpaid wages due and owing to Ellis any alleged payment was not supervised by the Department of Labor or any court.

The untimely payment of overtime wages, in itself, does not resolve a claim for unpaid wages under the law. See, e.g., Seminiano v. Xyris Enterp., Inc., 602 Fed.Appx. 682, 683 (9th Cir. 2015); Lynn's Food Stores, Inc. v. United States, 679 F.2d 1350, 1352-54 (11th Cir. 1982).

Nor does the untimely payment of wages, if any, compensate workers for the damages they incurred due to Cargill Meat Solutions's acts and omissions resulting in the unpaid wages in the first place.

Plaintiff, Eric Ellis remains uncompensated for the wages and other damages owed by Cargill Meat Solutions under federal law.

Like many other companies across the United States, Cargill Meat Solution's timekeeping and payroll systems were affected by the hack of Kronos in 2021.

That hack led to problems in timekeeping and payroll throughout Cargill's organization.

As a result, Cargill's employees who were not exempt from overtime under federal law were not paid for all overtime hours worked or were not paid their proper overtime premium after the onset of the Kronos hack.

Eric Ellis is one such Cargill worker.

Cargill could have easily implemented a system to accurately record time and properly pay non-exempt hourly and salaried employees until issues related to the hack were resolved.

But it didn't. Instead, Cargill Meat Solutions used prior pay periods or reduced payroll estimates to avoid paying wages and proper overtime to these nonexempt hourly and salaried employees.

Cargill Meat Solutions pushed the cost of the Kronos hack onto the most economically vulnerable people in its workforce.

Cargill Meat Solutions made the economic burden of the Kronos hack fall on front-line workers—average Americans—who rely on the full and timely payment of their wages to make ends meet.

Cargill's failure to pay wages, including proper overtime, for all hours worked violates the Fair Labor Standards Act (FLSA), 29 U.S.C. § 201, et seq.

Eric Ellis brings this lawsuit to recover these unpaid overtime wages and other damages owed by Cargill Meat Solutions because in reality he was the victim of not just the Kronos hack, but Cargill's decision to make its own non-exempt employees workers bear the economic burden for the hack.

Plaintiff Eric Ellis allege the following against Cargill Meat Solutions based upon the investigation of public information and personal experiences during his employment with Cargill.

COUNT V

Fair Labor Standards Act – Overtime Violations

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

Plaintiff incorporates by reference the allegations set forth above.

The FLSA requires that covered employees receive compensation for all hours worked and overtime compensation not less than one and one-half times the regular rate of pay for all hours worked in excess of forty hours in a work week. 29 U.S.C. § 207(a)(1).

At all times material herein, Plaintiff is covered employees entitled to the rights, protections, and benefits provided under the FLSA. 29 U.S.C. §§ 203(e) and 207(a).

Defendant is covered employers required to comply with the FLSA's mandates.

Defendant violated the FLSA with respect to Plaintiff, by, inter alia, failing to compensate Plaintiff for all hours worked and, with respect to such hours, failing to pay the legally mandated overtime premium for such work, as well as failing to provide compensation that is unconditional, free, and clear of deductions and/or kickbacks as described herein. Defendant also

violated the FLSA by failing to keep required, accurate records of all hours worked by Plaintiff. 29 U.S.C. § 211(c).

Plaintiff is a victim of uniform and company-wide compensation policies instituted individually and separately by each Defendant. These uniform policies, in violation of the FLSA, are applied to current and former non-exempt, hourly laborers working throughout the United States, including in the State of Texas.

Defendant required Plaintiff to perform work before he clock in, i.e., using the manual time clock sheets since the Kronos "Ransomware Attack". Defendant also required Plaintiff to incur uncompensated "waiting time" hours. Defendant also manipulated Plaintiff's time records to fraudulently misrepresent the actual number of hours worked, depriving Plaintiff of compensation for all overtime hours worked.

Defendant has not paid and continues to refuse to pay Plaintiff overtime for all hours worked beyond 40 in each work week.

Upon information and belief, Defendant Cargill Meat Solution's violative overtime practices occur in a similar fashion across its numerous job sites around the United States.

Upon information and belief, Defendant Cargill's violative overtime practices occur in a similar fashion across multiple job sites around the State of Texas.

Plaintiff is entitled to damages equal to the mandated pay, including minimum wage, straight time, and overtime premium pay within the three years preceding the filing of the complaint, plus periods of equitable tolling, because Defendant have acted willfully and knew or showed reckless disregard for whether the alleged conduct was prohibited by the FLSA.

Defendant, and each of them, have acted neither in good faith nor with reasonable grounds to believe that their actions and omissions were not a violation of the FLSA, and as a result thereof, Plaintiff is entitled to recover an award of liquidated damages in an amount equal to the amount of unpaid overtime pay and/or prejudgment interest at the applicable rate. 29 U.S.C. § 216(b).

Defendant Cargill Meat Solutions, willfully violated and continue to willfully violate the FLSA, by having engaged and continuing to engage in conduct which demonstrates a willful and/or reckless disregard for the provisions of the FLSA. Plaintiff spoke with managers or officers of Cargill Meat Solutions to alert them of the wage violations. Cargill was therefore on notice of their FLSA obligations and did not correct the violative practices.

As a result of the aforesaid violations of the FLSA's provisions, pay, including minimum wage, straight time, and overtime compensation, has been unlawfully withheld by Defendant from Plaintiff. Accordingly, Defendant is liable for unpaid wages, together with an amount equal as liquidated damages, attorneys' fees, and costs of this action.

Defendant violated the FLSA with respect to Plaintiff, by, inter alia, failing to compensate Plaintiff for all hours worked and, with respect to such hours, as well as failing to provide compensation that is unconditional, free, and clear of deductions and/or kickbacks as described herein. Defendant also violated the FLSA by failing to keep required, accurate records of all hours worked by Plaintiff and other employees. 29 U.S.C. § 211(c).

Defendant diluted Plaintiff's regular hourly rates of pay below the minimum wage by fabricating, underreporting or otherwise artificially reducing the total hours reported worked by Plaintiff.

As a result, Defendant improperly diluted Plaintiff's regular hourly rates of pay and has not compensated Plaintiff for all hours worked.

Defendant have not paid and continue to refuse to pay Plaintiff for all hours worked during each work week.

Defendant violated the FLSA minimum wage by not properly compensating Plaintiff for all hours worked in a work week, thereby diluting his regular hourly rate.

Defendant's wage violations were and are willful.

As a result of Defendant's violations of the FLSA, Plaintiff is entitled to recover unpaid wages dating three (3) years from the date of this filing of this Complaint, plus an additional equal amount in liquidated damages, reasonable attorneys' fees, and costs of this action. Wherefore, Plaintiff request relief as hereinafter provided. As a direct and proximate result of Defendant's actions, Plaintiff have been and continue to be damaged, suffering economic harm, lost earnings and benefits, and other damages.

Defendant is liable to Plaintiff for civil penalties, damages, compensatory damages, and other relief including but not limited to injunctive relief, and all costs and attorneys' fees incurred in this action.

Wherefore, Plaintiff request relief as hereinafter provided.

COUNT VI

Breach of Contract

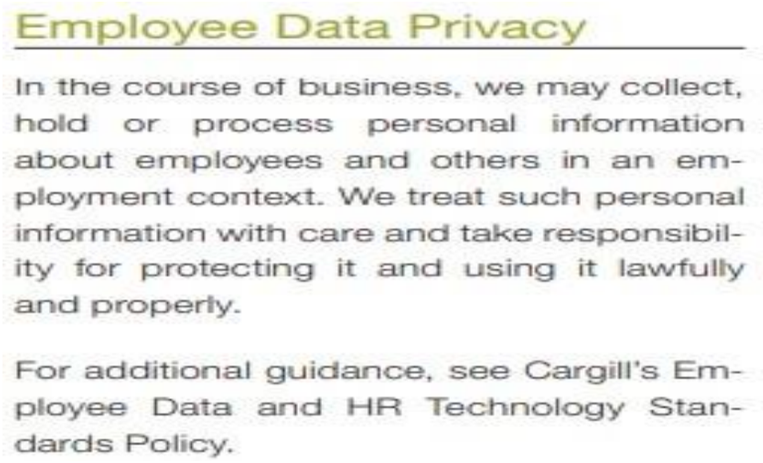
(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

Plaintiff incorporates by reference the allegations contained in each and every paragraph of this Complaint. At all relevant times, Cargill Meat Solutions and Cargill's employees mutually assented to and therefore were bound by the employment contract, Privacy Policy and Security Policy (the "Contract") that was operative at the time Plaintiff was employed by Cargill. Cargill stated on its website, in its "Cargill Data Privacy Principles" "We protect it against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, using appropriate technical and organizational measures." The contract was breached when the Plaintiff's Data was breached due to a "ransomware attack" on Kronos. The contract was also breached when the Plaintiff was not paid for actual hours worked.

The contract was also breached when Eric Ellis was discriminated against several times and retaliated against for being in a protected class.

Page 3 of code of conduct

Cargill affirmatively stated in the Employee Handbook that it shares Employment Information with authorized Third-Party Service Providers, such as compensation and benefits providers that have a "need to know" that information. Where it does so, Cargill imposes appropriate contractual obligations regarding Employment Information on such Third-Party Providers.



Employee Data Privacy

In the course of business, we may collect, hold or process personal information about employees and others in an employment context. We treat such personal information with care and take responsibility for protecting it and using it lawfully and properly.

For additional guidance, see Cargill's Employee Data and HR Technology Standards Policy.

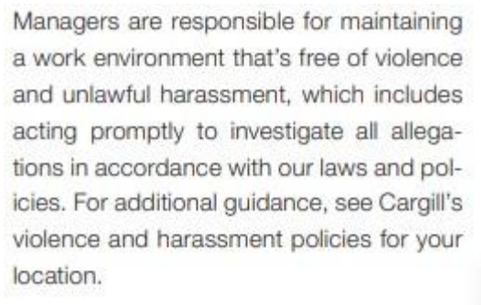
page 13 of the code of conduct

page 17 of the Cargill's code of conduct

Cargill Meat Solutions breached the Contract by failing to adequately screen its 3rd party service providers in which it shares its employees sensitive PII to ensure it have proper safeguards to protect the Plaintiff's PII and allowing a malicious third party to access that information without permission. The Defendant have violated its commitment to maintain the confidentiality and security of the PII of Plaintiff and failed to comply with their own polices and industry standards related to data security.

page 27 of the employee handbook

Cargill Meat Solutions breached the contract by subjecting Eric Ellis to discriminatory conduct including but not limited to sexual harassment.



Managers are responsible for maintaining a work environment that's free of violence and unlawful harassment, which includes acting promptly to investigate all allegations in accordance with our laws and policies. For additional guidance, see Cargill's violence and harassment policies for your location.

In the employee Handbook it states that Managers are responsible for maintaining a work environment that's free of unlawful harassment. Defendant Cargill Meat Solutions breached the contract by subjecting the Plaintiff to sexual harassment by a Cargill Supervisor. Cargill Supervisor Mike Calixto sexually harassed the Plaintiff Eric Ellis along with Senior Oven Operator Brian George.

Harassment and Violence

We all have a right to work in an environment that's free from violence or harassment. At Cargill, we will not tolerate:

- Harassment in any form
- The use of physical force intended to cause bodily harm
- Acts or threats that are intended to intimidate someone or cause them to fear bodily harm

This applies to the way we treat each other and anyone else we interact with. Each of us is responsible for conducting ourselves in a manner consistent with our harassment and violence policies.

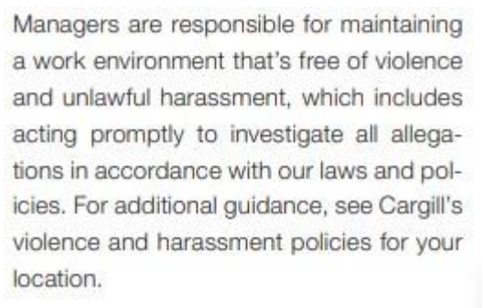
Page 25 of the Cargill code of conduct

COUNT VII

BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

Plaintiff incorporate by reference the allegations contained in each and every paragraph of this Complaint. Plaintiff entered contracts with Cargill, the Cargill code of conduct Policy, states managers are responsible for maintaining a work environment that's free of unlawful harassment which included the implied terms that Cargill's supervisors would not cause discrimination or retaliate against the Plaintiff for complaining of such discriminatory treatment.


Managers are responsible for maintaining a work environment that's free of violence and unlawful harassment, which includes acting promptly to investigate all allegations in accordance with our laws and policies. For additional guidance, see Cargill's violence and harassment policies for your location.

In this contract, as in every contract, there was an implied covenant of good faith and fair dealing. This implied promise means that each party will not do anything to unfairly interfere with the right of any other party to receive the benefits of the contract. Good faith means honesty of purpose without any intention to mislead or to take unfair advantage of another, that is, being faithful to one's duty or obligation.

Plaintiff performed everything that he was required to do under the contract arriving to work and working for Cargill Meat Solutions. Cargill Meat Solutions ignored Eric Ellis's sexual harassment complaints forcing him to continue working with the harassers resulting in consecutive sexual harassment events. Cargill's actions and/ or inactions were done maliciously and willing.

By doing so, Cargill Meat Solutions did not act fairly and in good faith.

As a result of this conduct, the Plaintiff was damaged.

COUNT VIII

DISCRIMINATION

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

Plaintiff restates and realleges the allegations contained in all paragraphs of this complaint as though set forth here in full.

Plaintiff was an employees of Cargill within the meaning of 42 U.S.C. § 2000(e) et seq.

The discriminatory policies or practices of Cargill, as set forth in this Complaint, have denied Plaintiff his right to equal employment opportunity in violation of 42 U.S.C. § 2000(e) et seq

Plaintiff Eric Ellis asserts the following claim of discrimination.

Plaintiff restates and realleges the allegations contained in the Paragraphs above of this Complaint as though set forth here in full.

Plaintiff has experienced race and sex discrimination with respect to the racially motivated drug tests of Eric Ellis, racially and sexually motivated harassment, and retaliation for complaining about workplace harassment, resulting in the discharge of the plaintiff.

Cargill's wrongful conduct towards Plaintiff was intentional, malicious, deliberate, willful and oppressive, and was carried out with reckless and callous disregard for his rights.

By reason of Cargill's discriminatory and unlawful employment practices as set forth in this Complaint, Plaintiff has suffered damage including, but not limited to, lost income, lost benefits, embarrassment, emotional distress, physical injury, humiliation, indignity and a reduced quality of life.

COUNT VIIII

RETALIATION

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

Ellis incorporates by reference in all paragraphs of this complaint.

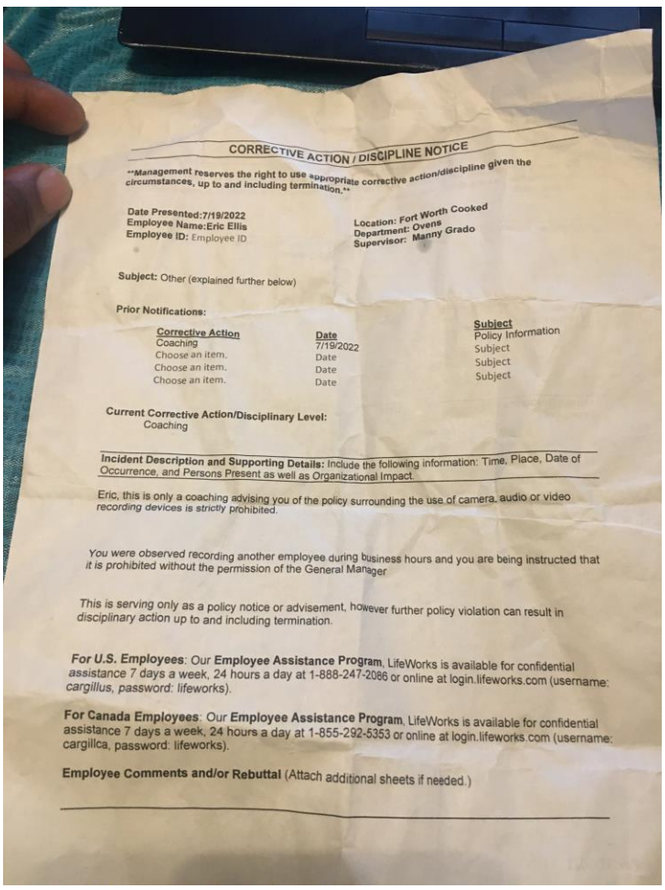
Cargill Meat Solutions Defendants retaliated against Ellis for the complaint by his regarding Cargill's Supervisors sexual misconduct by:

(a) materially disciplining Eric Ellis for recording the sexual harassment he experienced by the Defendant's supervisors;

(b) materially increasing the scrutiny of Eric Ellis;

(c) materially falsely accusing Eric Ellis of wrong doing

(d) implementing and maintaining hostile work conditions compelling Ellis to terminate his employment or otherwise constructively discharging Ellis.



CORRECTIVE ACTION / DISCIPLINE NOTICE

Management reserves the right to use appropriate corrective action/discipline given the circumstances, up to and including termination.

Date Presented:7/19/2022
Employee Name:Eric Ellis
Employee ID: Employee ID

Location: Fort Worth Cooked
Department: Ovens
Supervisor: Manny Grado

Subject: Other (explained further below)

Prior Notifications:

Corrective Action	Date	Subject
Coaching	7/19/2022	Policy Information
Choose an item.	Date	Subject
Choose an item.	Date	Subject
Choose an item.	Date	Subject

Current Corrective Action/Disciplinary Level:
Coaching

Incident Description and Supporting Details: Include the following information: Time, Place, Date of Occurrence, and Persons Present as well as Organizational Impact:

Eric, this is only a coaching advising you of the policy surrounding the use of camera, audio or video recording devices is strictly prohibited.

You were observed recording another employee during business hours and you are being instructed that it is prohibited without the permission of the General Manager

This is serving only as a policy notice or advisement, however further policy violation can result in disciplinary action up to and including termination.

For U.S. Employees: Our Employee Assistance Program, LifeWorks is available for confidential assistance 7 days a week, 24 hours a day at 1-888-247-2086 or online at login.lifeworks.com (username: cargillus, password: lifeworks).

For Canada Employees: Our Employee Assistance Program, LifeWorks is available for confidential assistance 7 days a week, 24 hours a day at 1-855-292-5353 or online at login.lifeworks.com (username: cargillca, password: lifeworks).

Employee Comments and/or Rebuttal (Attach additional sheets if needed.)

As a consequence of the retaliation, Ellis suffered tangible adverse employment actions including:

(a) loss of back pay;

(b) loss of forward pay;

(c) physical injuries, pain and suffering;

(d) emotional harm;

(e) liability for healthcare expenses which otherwise would have been covered by the healthcare insurance provided by Cargill Meat Solutions;

(f) other damages.

COUNT X

CONSPIRACY TO VIOLATE CIVIL RIGHTS UNDER 42 U.S.C. §J985(3)

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

By their actions described above, Cargill Meat Solutions conspired and acted with animus towards Ellis as a homosexual black male worker with the purpose of hindering and preventing Federal and state officials from performing their affirmative obligations to Ellis, including but not limited to the obligations of these officials to ensure that all constructively

discharged employees be entitled to unemployment compensation. The Defendants failed to keep accurate records and submitted altered records to influence the Texas Workforce Commission to deny the Plaintiff the benefits of Unemployment.

Ellis has been injured in his person and property and has been deprived of rights and privileges guaranteed by the laws and the Constitution of the United States.

The acts and conduct of Cargill Meat Solutions constitute a conspiracy to violate Ellis's civil rights under 42 U.S.C. § 1985(3).

The acts and conduct of Cargill Meat Solutions constitute a conspiracy to violate Ellis's civil rights under 42 U.S.C. § 1985(3).

COUNT XI

VIOLATIONS OF TEXAS LABOR CODE § 21.051(1)

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

The acts and conduct of Cargill Meat Solutions violated Texas Labor Code § 2l.051(1).

As a consequence of violations of Texas Labor Code § 21.051(1), Ellis sustained actual damages including:

(a) loss of back pay;

(b) loss of front pay;

(c) physical injuries, pain and suffering;

(d) emotional harm;

(e) liability for past healthcare expenses, which otherwise would have been covered by the healthcare insurance provided by Cargill Meat Solutions;

(f) liability for future healthcare expenses, which otherwise would have been covered by the healthcare insurance provided by Cargill Meat Solutions; and

(g) other damages.

COUNT XII

VIOLATIONS OF TEXAS LABOR CODE § 21.056

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

The acts and conduct of Cargill Meat Solutions violated Texas Labor Code §21.056 in that Cargill abetted, incited and coerced its employees to engage in discriminatory practices against Ellis.

As a direct and proximate cause of the violations of Texas Labor Code §21.056, Ellis sustained actual damages, including:

(a) loss of back pay;

(b) loss of front pay;

(c) physical injuries, pain and suffering;

(d) emotional harm;

(e) liability for past healthcare expenses, which otherwise would have been covered by the healthcare insurance provided by Cargill Defendants;

(f) liability for future healthcare expenses, which otherwise would have been covered by the healthcare insurance provided by Cargill Defendants; and (g) other damages.

COUNT XIII

VIOLATIONS OF TEXAS TORT LAW

Negligent Hiring and Retention

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

Defendant Cargill Meat Solutions knew or reasonably should have known that at the time they hired Supervisor Yanet Hernandez that she would retaliate against the Plaintiff if she was paired with harasser Supervisor Mike Calixto.

Cargill negligently employed and/or retained the employment of several of their supervisors and facilitated the sexual harassment of the plaintiff.

As a direct and proximate cause of Cargill's negligence, Eric Ellis sustained actual damages consisting of:

(a) Physical injuries, pain and suffering;

(b) Emotional harm;

(c) Past health care expenses, which otherwise would have been covered by the healthcare insurance provided by Cargill Meat Solutions; and

(d) Future healthcare expenses, which otherwise would have been covered by the healthcare insurance provided by Cargill Meat Solutions.

COUNT IX

INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS

(AGAINST DEFENDANT CARGILL MEAT SOLUTIONS)

The acts and conduct of Defendant Cargill constitute the intentional infliction of emotional harm upon Plaintiff Eric Ellis.

As a consequence of the intentional infliction of emotional harm by upon Ellis be Cargill. Cargill failed to properly address the sexual harassment after the first complaint of sexual harassment, allow Plaintiff Eric Ellis to subjected to more instances of harassment based on his orientation. Ellis sustained actual damages, including without limitation the following:

(a) Physical injuries, pain and suffering;

(b) Past emotional suffering;

(c) Future emotional suffering;

(d) Past medical expenses, which otherwise would have been covered by the healthcare insurance provided by Cargill;

(e) Future medical expenses, which otherwise would have been covered by the healthcare insurance provided by Defendant Cargill; and

(f) Other actual damages.

DAMAGES

Compensatory Damages

(Under Federal Law)

As a consequence of the acts and conduct of Defendant Cargill's supervisors, Ellis has sustained actual damages including without limitation the following:

(a) Past Loss Wages in a sum not less than $22,9090;

(b) Future Loss wages - $2,495,988;

(c) Past healthcare expenses - $915.00;

(d) Past physical pain, as may reasonably be determined by the court and jury;

(e) Future physical pain, as may reasonably be determined by the court and Jury; (f) Past emotional suffering, as may reasonably be determined by the court and jury;

(g) Future emotional suffering, as may reasonably be determined by the court and jury.

Compensatory Damages

(Under Texas Labor Code)

As a consequence of the acts and conduct of Defendant, Ellis has sustained actual damages within the context of Texas Labor Code §21.2585(l) including without limitation the following:

(a) Past Loss Wages in a sum not less than $22,9090;

(b) Future Loss wages - $2,495,988;

(c) Past healthcare expenses - $915.00;

(d) Past physical pain, as may reasonably be determined by the court and jury;

(e) Future physical pain, as may reasonably be determined by the court and Jury; (f) Past emotional suffering, as may reasonably be determined by the court and jury;

(g) Future emotional suffering, as may reasonably be determined by the court and jury.

Punitive Damages

(Under Federal Law)

Cargill's acts and conduct is so reprehensible to warrant the imposition of further sanctions to achieve punishment or deterrence.

In addition to all other relief to which Ellis is entitled, Ellis is entitled to punitive damages reasonable in relationship to the actual damages and considering:

(a) the actual harm sustained by Ellis;

(b) the indifference to or reckless disregard by Defendant Cargill of Ellis's mental health and safety;

(c) the repetitiveness of the acts and conduct which directly and proximately caused the actual damages of Ellis;

(d) the harm occasioned to Ellis as a consequence of the discrimination by Cargill of Ellis's sexual orientation; and

(e) other relevant considerations in accordance with law.

Punitive Damages

(Under Texas Labor Code)

In addition to all other relief to which Ellis is entitled, Ellis is entitled to punitive damages against Cargill Meat Solutions pursuant to Texas Labor Code §21.2585(a)(2).

Punitive Damages

Under Tex.Civ.Prac.& Rem. Code §41.003(2)

In addition to all other relief to which Ellis is entitled, Ellis is entitled to punitive damages against Defendant Cargill Meat Solutions pursuant to Tex.Civ.Prac.& Rem. Code §41.003.

OTHER RELIEF

Damages stemming from the FLSA violations.

In addition to all other relief to which Ellis is entitled, he is entitled to prejudgment interest upon his actual damages as well as future damages in accordance with law.

CLAIMS FOR RELIEF AGAINST UKG

COUNT I

NEGLIGENCE

Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

Given the highly sensitive nature of the PII UKG collects from its employees and the likelihood of harm resulting from its unauthorized access, acquisition, use, or disclosure, UKG owes Plaintiff a duty to exercise reasonable care in protecting this information. This duty includes implementing and maintaining reasonable security procedures and practices appropriate to the nature of the PII that were compliant with and/or better than industry-standard practices. UKG's duties included a duty to design, maintain, and test its security systems to ensure that Plaintiff's PII was adequately secured and protected, to implement processes that would detect a breach of its security system in a timely manner, to timely act upon warnings and alerts, including those generated by its own security systems regarding intrusions to its networks, and to promptly, properly, and fully notify its customers, Plaintiff, of any data breach.

It was foreseeable by UKG that a failure to use reasonable measures to protect the highly sensitive and confidential information of its customers' employees could result in injury to said employees.

Actual and attempted breaches of data security were reasonably foreseeable to UKG given that other payroll companies had recently been breached before as well as the known frequency of data breaches and various warnings from industry experts.

In connection with the conduct described above, UKG acted wantonly, recklessly, and with complete disregard for the consequences Plaintiff would suffer if his highly sensitive and confidential PII, including but not limited to name, company name, address, email address, time and attendance and schedule information, and Social Security Numbers, was accessed by unauthorized third parties.

UKG had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff would be harmed by the failure to protect his PII

because hackers routinely attempt to steal such information and use it for nefarious purposes, but UKG also knew that it was more likely than not Plaintiff would be harmed.

UKG's duty also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as UKG.

Various FTC publications and data security breach orders further form the basis of UKG's duty. According to the FTC, the need for data security should be factored into all business decision making.

In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. Among other things, the guidelines note that businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

UKG's duty also arose from its unique position as one of the largest cloud computing companies in the world whose services constitute a linchpin of the payroll services of a substantial fraction of the nation. As set forth above, the data breach herein affected thousands of companies and millions of employees. UKG undertakes its collection of sensitive PII of employees generally through direct relationships between UKG and employers, generally without the direct consent of employees who have no

option but to be affected by UKG's actions. Plaintiff couldn't "opt out" of UKG's activities. UKG holds itself out as a trusted steward of consumer and employee data, and thereby assumed a duty to reasonably protect that data. Plaintiff, and indeed the general public, collectively repose a trust and confidence in UKG to perform that stewardship carefully. Otherwise, consumers and employees would be powerless to fully protect their interests regarding their PII, which is controlled by UKG. Because of its crucial role within the payroll system, UKG was in a unique and superior position to protect against the harm suffered by Plaintiff as a result of the UKG data breach. By obtaining, collecting, using, and deriving a benefit from Plaintiff's PII, UKG assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's PII from disclosure.

UKG admits that it has an enormous responsibility to protect employee data, that it is entrusted with this data, and that it did not live up to its responsibilities to protect the PII at issue here.

UKG's privacy policy has a specific "Security" section which states:

To prevent unauthorized access or disclosure, to maintain data accuracy, and to allow only the appropriate use of your PII, UKG utilizes physical, technical, and administrative controls and procedures to safeguard the information we collect.

To protect the confidentiality, integrity, availability and resilience of your PII, we utilize a variety of physical and logical access controls, firewalls, intrusion detection/prevention systems, network and database monitoring, anti-virus, and backup systems. We use encrypted sessions when collecting or transferring sensitive data through our websites.

We limit access to your PII and data to those persons who have a specific business purpose for maintaining and processing such information. Our employees who have been granted access to your PII are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided with training and instruction on how to do so.

Timely notification was required, appropriate, and necessary so that, among other things, Plaintiff could take appropriate measures to freeze or

lock his credit profiles, cancel or change usernames or passwords on compromised accounts, monitor his account information and credit reports for fraudulent activity, contact his banks or other financial institutions that issue his credit or debit cards, obtain credit monitoring services, develop alternative timekeeping methods or other tacks to avoid untimely or inaccurate wage payments, and take other steps to mitigate or ameliorate the damages caused by UKG's misconduct.

UKG also owed a duty to the Plaintiff to exercise reasonable care to avoid sudden disruption of their human resources services, including their timekeeping and payroll services. UKG undertook of its own volition responsibility to provide continuous and ongoing timekeeping and payroll services to the employers of Plaintiff, knowing that such services were for the benefit of making timely wage payments to them, among other things, and that any disruption, particularly any sudden disruption, would cause Plaintiff harm.

UKG breached the duties it owed to Plaintiff described above and thus was negligent. UKG breached these duties by, among other things, failing to:

(a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff;

(b) prevent the breach;

(c) detect the breach while it was ongoing;

(d) maintain security systems consistent with industry standards and necessary to avoid the disabling of payroll systems for thousands of companies and millions of workers;

(e) disclose that Plaintiff's PII in UKG's possession had been or was reasonably believed to have been stolen or compromised; and (f) avoid disruption and continued disruption of its timekeeping and payroll services.

UKG knew or should have known of the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the increasing frequency of ransomware attacks on payroll vendors such as UKG.

Through UKG's acts and omissions described in this Complaint, including UKG's failure to provide adequate security and its failure to protect the PII of Plaintiff from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, UKG unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's PII. UKG further failed to timely and accurately disclose to customers and the employees of their customers that their PII had been improperly acquired, accessed and was available for sale to criminals on the dark web. Indeed, Plaintiff received no notice of the breach directly from UKG. UKG issued a public statement and in some instances issued notices to its customers (the employers of Plaintiff) but failed to adequately describe all types of PII that were exfiltrated, stolen, disclosed, or accessed by the ransomware attackers.

UKG further breached its duty to Plaintiff to exercise reasonable care to avoid sudden disruption of their human resources services, including their timekeeping and payroll services, by allowing its systems to remain disabled for multiple weeks (and counting) and failing to adequately and timely remedy its security vulnerabilities.

But for UKG's wrongful and negligent breach of its duties owed to Plaintiff, his PII would not have been compromised nor his timekeeping and payroll services disabled.

As a direct and proximate result of UKG's negligence, Plaintiff have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. As a result of UKG's failure to protect Plaintiff's PII, Plaintiff's PII has been accessed by malicious cybercriminals.

Plaintiff's injuries include:

a. damages stemming from Plaintiff not being fully paid for all time worked, not being paid overtime, being provided inaccurate wage statements or no wage statements at all, not being provided meal and rest breaks or compensation in lieu thereof, all in violation of federal and state laws;

b. damages stemming from the fear and anxiety of Plaintiff concerning whether he would be fully, timely, and accurately paid for all

time worked during the 2021-2022 holiday season, and regarding how long such disruptions to his payroll systems would continue;

c. theft of his PII;

d. costs associated with requested credit freezes;

e. costs associated with the detection and prevention of identity theft and unauthorized use of his financial accounts;

f. costs associated with purchasing credit monitoring and identity theft protection services;

g. unauthorized charges and loss of use of and access to his financial account funds and costs associated with the inability to obtain money from his account or being limited in the amount of money he was permitted to obtain from his accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on his credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

j. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by his PII being placed in the hands of criminals;

k. damages to and diminution of value of his PII entrusted, directly or indirectly, to UKG with the mutual understanding that UKG would safeguard Plaintiff's data against theft and not allow access and misuse of his data by others;

l. continued risk of exposure to hackers and thieves of his PII, which remains in UKG's possession and is subject to further breaches so long as UKG fails to undertake appropriate and adequate measures to protect Plaintiff;

m. loss of the inherent value of his PII;

n. and other significant additional risks of identity theft, financial fraud, and other identity-related fraud in the indefinite future.

COUNT II

UNJUST ENRICHMENT

Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

Plaintiff has an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by UKG and that was ultimately converted, stolen, removed, deleted, exfiltrated, or disclosed in the UKG data breach. This PII was conferred on UKG in most cases by third parties, Plaintiff's employer, but in some instances directly by Plaintiff himself.

UKG was benefitted by the conferral upon it of the PII pertaining to Plaintiff and by its ability to retain and use that information. UKG understood that it was in fact so benefitted.

UKG also understood and appreciated that the PII pertaining to Plaintiff was private and confidential, and its value depended upon UKG maintaining the privacy, security, and confidentiality of that PII.

But for UKG's willingness and commitment to maintain its privacy, security, and confidentiality, that PII would not have been transferred to and entrusted with UKG. Further, if UKG had disclosed that its data security measures were inadequate, UKG would not have been permitted to continue in operation by regulators, its shareholders, and participants in the marketplace.

As a result of UKG's wrongful conduct as alleged in this Complaint (including among other things its failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiff without having adequate data security measures, and its other conduct in facilitating the theft of that PII), UKG has been unjustly enriched at the expense of, and to the detriment of, Plaintiff. Among other things, UKG has and continues to benefit and profit from the sale of the PII

and from its contracts to use that PII to process timekeeping and payroll, while the value to Plaintiff has been diminished.

UKG's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

Under the common law doctrine of unjust enrichment, it is inequitable for UKG to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff in an unfair and unconscionable manner. UKG's retention of such benefits under circumstances making such retention inequitable constitutes unjust enrichment.

The benefit conferred upon, received, and enjoyed by UKG was not conferred officiously or gratuitously, and it would be inequitable and unjust for UKG to retain the benefit.

UKG is therefore liable to Plaintiff for restitution in the amount of the benefit conferred on UKG as a result of its wrongful conduct, including specifically the value to UKG of the PII that was stolen and the payroll systems that were compromised in the UKG data breach and the profits UKG is receiving from the use, sale, and processing of that information, including any profits from its timekeeping and payroll services.

COUNT III

BREACH OF CONTRACT

Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

UKG's privacy policy is an agreement between UKG and its customers as well as the employees of its customers, who include Plaintiff, and who provided his PII to UKG.

This privacy policy applied to Plaintiff who accepted UKG's promise and entered into a contract with UKG when he entrusted highly sensitive and confidential e-PHI to UKG as part of a transaction for medical goods and services.

Plaintiff is entitled to compensatory and consequential damages as a result of UKG's breach of contract.

COUNT IV

COMMON LAW INVASION OF PRIVACY – INTRUSION UPON SECLUSION

Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

To assert claims for intrusion upon seclusion, one must plead

(1) that the defendant intentionally intruded into a matter as to which plaintiff had a reasonable expectation of privacy; and

(2) that the intrusion was highly offensive to a reasonable person.

UKG intentionally intruded upon the solitude, seclusion and private affairs of Plaintiff by intentionally configuring their systems in such a way that left them vulnerable to malware/ransomware attack, thus permitting unauthorized access to their systems, which compromised Plaintiff's PII. Only UKG had control over its systems.

UKG's conduct is especially egregious and offensive as they failed to have any adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiff's information.

At all times, UKG was aware that Plaintiff's PII in their possession contained highly sensitive and confidential PII, including but not limited to name, company name, address, email address, time and attendance and schedule information, and Social Security Numbers.

Plaintiff has a reasonable expectation in his e PHI, which contains highly UKG intentionally configured their systems in such a way that stored Plaintiff's PII to be left vulnerable to malware/ransomware attack without regard for Plaintiff's privacy interests.

The disclosure of the sensitive and confidential PII of hundreds of thousands of employees, was highly offensive to Plaintiff because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

UKG's conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive information, in addition to social norms. UKG's conduct would be especially egregious to a reasonable person as UKG publicly disclosed Plaintiff's sensitive and confidential PII, including but not limited to name, company name, address, email address, time and attendance and schedule information, and Social Security Numbers, without his consent, to an "unauthorized person," i.e., hackers.

As a result of UKG's actions, Plaintiff have suffered harm and injury, including but not limited to an invasion of his privacy rights.

The plaintiff has been damaged as a direct and proximate result of UKG's intrusion upon seclusion and is entitled to just compensation.

Plaintiff are entitled to appropriate relief, including compensatory damages for the harm to his privacy, loss of valuable rights and protections, and heightened risk of future invasions of privacy.

COUNT V

DEPRIVATION OF RIGHTS

Sec.19. OF THE TEXAS CONSTITUTION

Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

Sec 19 of the Texas Constitution provides: "No citizen of this State shall be deprived of life, liberty, property, privileges or immunities, or in any manner disfranchised, except by the due course of the law of the land." Sec 19. Texas. Const

The Krono's Data Breach allowed the deprivation of the Plaintiff's sensitive information.

COUNT VI

INVASION OF PRIVACY

> Texas recognizes a common law right to privacy. The Invasion of Privacy tort encompasses distinct violations of one's privacy such as: (1) intrusion upon one's solitude or private affairs;
>
> *Billings v. Atkinson*, 489 S.W.2d 858, 860 (Tex. 1973) (recognizing an intrusion of seclusion as a legal cause of action)

An invasion of privacy by intrusion upon one's solitude occurs when:

(1) there is "an intentional intrusion…upon the solitude, seclusion, or private affairs or concerns of another;"

(2) such an intrusion would be "highly offensive to a reasonable person;" and

(3) the intrusion caused an injury to the person whose privacy was violated. *Fawcett v. Grosu*, 490 S.W.3d 650, 664 (Tex. App.—Hous. [14th Dist.] 2016, pet. denied)

UKG violated Plaintiff's constitutional right to privacy by collecting, storing, and disclosing his PII in which they had a legally protected privacy interest, and in which they had a reasonable expectation of privacy in, in a manner that was highly offensive to Plaintiff, would be highly offensive to any reasonable person, and was an egregious violation of social norms.

UKG has intruded upon Plaintiff's legally protected privacy interests, including interests in precluding the dissemination or misuse of his confidential PII.

UKG's actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that:

(i) the invasion occurred within a zone of privacy protected by the Texas Constitution, namely the misuse of information gathered for an improper purpose; and

(ii) the invasion deprived Plaintiff of the ability to control the circulation of his PII, which is considered fundamental to the right to privacy.

Plaintiff had a reasonable expectation of privacy in that:

(i) UKG's invasion of privacy occurred as a result of UKG's security practices including the collecting, storage, and unauthorized disclosure of its customers' employees' PII;

(ii) Plaintiff did not consent or otherwise authorize UKG to disclosure his PII; and

(iii) Plaintiff could not reasonably expect UKG would commit acts in violation of laws protecting privacy.

As a result of UKG's actions, Plaintiff have been damaged as a direct and proximate result of UKG's invasion of his privacy and are entitled to just compensation.

The plaintiff suffered actual and concrete injury as a result of UKG's violations of his privacy interests. Plaintiff is entitled to appropriate relief, including damages to compensate them for the harm to his privacy interests, loss of valuable rights and protections, heightened risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

Plaintiff seeks appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff for the harm to his privacy interests as well as disgorgement of profits made by UKG as a result of its intrusions upon Plaintiff's privacy.

COUNT VII

Violation of the Texas Consumer Privacy Act,

HB 4518

Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

HB 4518, also known as the Texas Consumer Privacy Act, grants the plaintiff (consumer):

1.) The right to disclosure of personal information collected by a business.

2.) The right to delete certain personal information collected by a business.

3.) The right to disclosure of certain personal information sold or disclosed by a business.

The TCPA would impose civil penalties in the amount of $2,500 for each violation or $7,500 for each intentional violation. The Act also gives the Attorney General the ability to restrain an alleged violation of the Act, after a 30-day notice period, by filing a temporary restraining order or a permanent or temporary injunction. The bill would not provide for a private cause of action.

UKG knew or should have known that its computer systems and data security practices were inadequate to safeguard the Plaintiff's PII and that the risk of a data breach or theft was highly likely. UKG failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Plaintiff's PII. Specifically, UKG subjected Plaintiff's nonencrypted and nonredacted PII to an unauthorized access and exfiltration, theft, or disclosure as a result of the UKG's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

As a direct and proximate result of UKG's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's PII included exfiltration, theft, or disclosure through UKG's servers, systems, and website, and/or the dark web, where hackers further disclosed UKG's customers' and their employees' PII.

As a direct and proximate result of UKG's acts, Plaintiff was injured and lost money or property, including but not limited to lost wages due to the disabling of his payroll and timekeeping services, the loss of Plaintiff's legally protected interest in the confidentiality and privacy of his PII, nominal damages, and additional losses described above.

COUNT VIII

REQUEST FOR RELIEF UNDER THE DECLARATORY JUDGMENT ACT

Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

An actual controversy has arisen in the wake of the data breach regarding UKG'S present and prospective common law and statutory duties to reasonably safeguard Plaintiff's personal information and whether UKG is currently maintaining data security measures adequate to protect Plaintiff from further data breaches. Plaintiff alleges that UKG's data security practices remain inadequate.

Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that UKG continues to owe a legal duty to secure consumers' PII, to timely notify Plaintiff of any data breach, and to establish and implement data security measures that are adequate to secure Plaintiff's PII.

The Court also should issue corresponding prospective injunctive relief requiring UKG to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's PII.

PRAYER FOR RELIEF

Wherefore, the Plaintiff respectfully requests that this Court:

A. Grant a permanent injunction enjoining the Defendant, Cargill Meat Solutions, its officers, successors, assigns, and all persons in active concert or participation with it, from engaging in any employment practice which discriminates on the basis of sex, or which facilitates, condones or encourages sexual harassment.

B. Order the Defendant to institute and carry out policies, practices, and programs which provide equal employment opportunities and a non-hostile

work environment for all employees, including males, and which eradicate the effects of its past and present unlawful employment practices.

C. Order the Defendant to make whole Eric Ellis a by providing appropriate back pay with prejudgment interest in amounts to be determined at trial, pecuniary losses, compensatory damages including out-of-pocket expenses, and other affirmative relief necessary to eradicate the effects of its unlawful employment practices.

D. Order the Defendant to make Eric Ellis whole by providing compensation for past and future pecuniary losses resulting from the unlawful employment practices, including but not limited to out-of-pocket job-hunting expenses.

E. Order the Defendant to make Eric Ellis whole by providing compensation for past and future nonpecuniary losses resulting from the unlawful employment practices including but not limited to, pain and suffering, humiliation, embarrassment, emotional distress, anxiety, and loss of enjoyment of life, in amounts to be determined at trial.

F. Order the Defendant to pay Eric Ellis punitive or exemplary damages for its intentional, malicious conduct or reckless indifference, in an amount to be determined at trial.

G. Grant such further relief as the Court deems necessary and proper in the public interest.

Plaintiff, on behalf of himself, requests the Court enter judgment against Cargill Meat Solutions:

a) An order enjoining Defendant from further unfair and deceptive business practices regarding the maintenance and protection of Cargill's Employees' sexual orientation and race;

c) An award to Plaintiff for nominal, consequential, statutory compensatory, punitive, exemplary, and statutory damages, including interest, in an amount to be proven at trial;

d) A declaration that the Defendant must make full restitution to Plaintiff;

e) An award of pre-judgment and post-judgment interest, as provided by law;

f) For an order finding Cargill Meat Solutions liable for violations of federal wage laws with respect to Ellis,

g) For a judgment awarding all unpaid wages, liquidated damages, and penalties, to Ellis;

h) For a judgment awarding costs of this action to Ellis;

i) For a judgment awarding pre- and post-judgment interest at the highest rates allowed by law to Ellis;

j) For all such other and further relief as may be necessary and appropriate.

JURY TRIAL DEMAND

The Plaintiff requests a jury trial on all questions of fact raised by his Complaint.

Respectfully submitted,

Eric L Ellis
8539 Melissa Dr
Fort Worth, Tx 76108
3185075030
EricLamarEllis@gmail.com

5.11.2023